Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

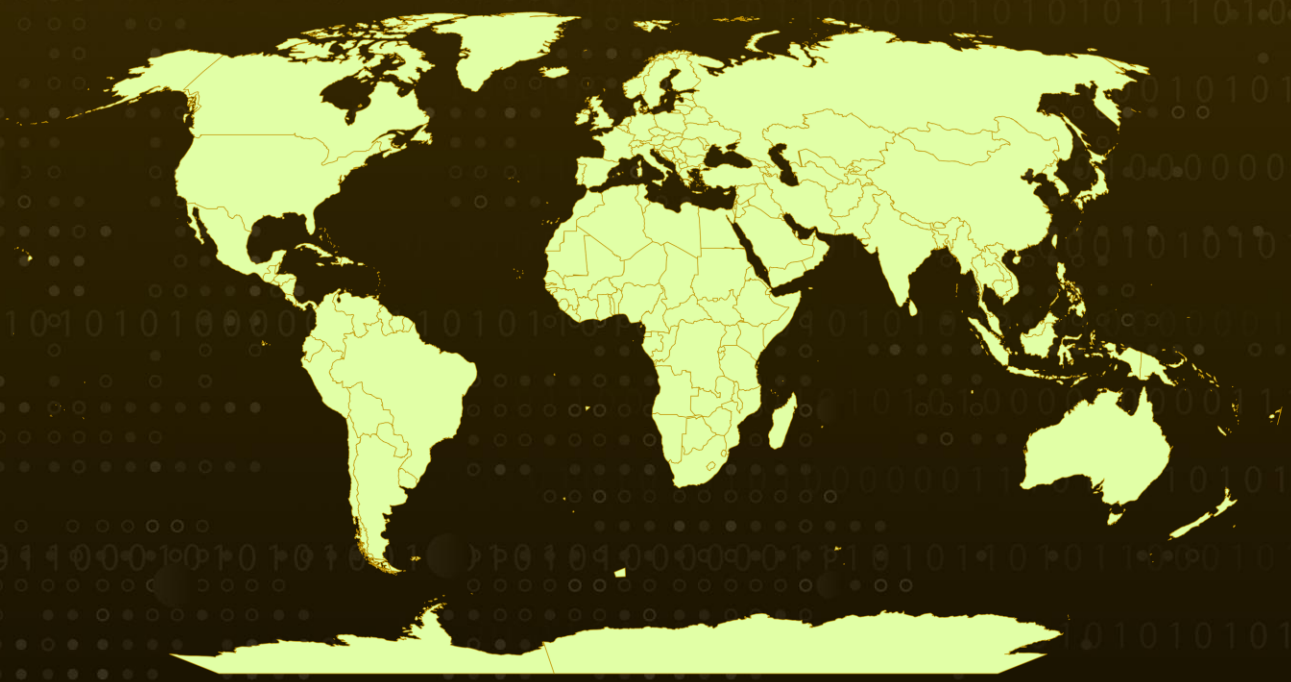
Crysis Threat Actors Unleash Venus Ransomware via RDP

Date of Publication	Admiralty Code	TA Number
July 07, 2023	A1	TA2023290

Summary

First appeared: 2016
Malware: Crysis and Venus ransomware
Attack Region: Worldwide
Affected platforms: Microsoft Windows
Attack: The threat actors behind the Crysis ransomware are currently utilizing the Venus ransomware as a component of their attack strategy, with a primary focus on targeting vulnerable systems through active Remote Desktop Protocol (RDP).

Attack Regions



Attack Details

#1 The malicious actors behind the Crysis ransomware were scouring the internet using brute force or dictionary attacks, in search of vulnerable Remote Desktop Protocol (RDP) endpoints to implant the Venus ransomware onto targeted systems. Once they successfully gained access, the attackers initially attempted to encrypt the compromised systems using the Crysis ransomware.

#2 However, if the encryption with Crysis failed, they resorted to a secondary encryption attempt using the Venus ransomware. In the event that the files are encrypted by the Crysis ransomware, the victims are presented with a ransom note containing an onion email address, which they can use to establish contact with the malevolent threat actors.

#3 After gaining control of the system through Remote Desktop Protocol (RDP), the threat actor utilizes NirSoft tools to scan the network and determine whether the compromised system is part of a specific network. Additionally, Mimikatz is employed to extract account credentials, aiding in internal reconnaissance and facilitating the encryption of additional systems within the network. Leveraging the acquired account information makes lateral movement feasible, providing access to other interconnected systems in the network.

Recommendations

To minimize the risk of attacks, it is advisable to disable RDP services over the Internet. Even If necessarily required, Enable Remote Desktop Protocol (RDP) services for a limited time and limited purpose. Furthermore, it is crucial to employ strong and regularly updated passwords for RDP accounts to thwart brute-force attacks.

Implement Multi-Factor Authentication (MFA) on all devices and systems to add an extra layer of security. Regularly monitor RDP server logs to promptly identify any suspicious activities. Ensure systems and software are kept up to date to benefit from the latest security enhancements and safeguard against emerging vulnerabilities.

Deploy firewalls and IDS to filter and monitor incoming RDP traffic, blocking unauthorized access attempts and detecting potential threats. Limit RDP access by restricting it exclusively to authorized users and devices, utilizing access control measures like IP whitelisting or VPN tunnels.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	TA0040 Impact	T1036 Masquerading
T1021 Remote Services	T1021.001 Remote Desktop Protocol	T1486 Data Encrypted for Impact	T1007 System Service Discovery
T1033 System Owner/User Discovery	T1595 Active Scanning	T1047 Windows Management Instrumentation	T1053 Scheduled Task/Job
T1059 Command and Scripting Interpreter	T1129 Shared Modules	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1134 Access Token Manipulation	T1027 Obfuscated Files or Information
T1027.005 Indicator Removal from Tools	T1070 Indicator Removal	T1070.004 File Deletion	T1140 Deobfuscate/Decode Files or Information
T1497 Virtualization/Sandbox Evasion	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1564 Hide Artifacts
T1564.003 Hidden Window	T1056 Input Capture	T1012 Query Registry	T1057 Process Discovery
T1490 Inhibit System Recovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	67b1a741e020284593a05bc4b1a3d218, 786ce74458720ec55b824586d2e5666d, 51373c09f0cb65ab149b0423d85f057e, 4984b907639851dfa8409e60c838e885, 8d0a0f482090df08b986c7389c1401c2, 3a302cd820b1535ccc6545542bf987d1, 57445041f7a1e57da92e858fc3efeabe, cc2d70a961bc6dce79168ae99ab30673, d28f0cfae377553fcb85918c29f4889b, 2a541cb2c47e26791bca8f7ef337fe38, 7f31636f9b74ab93a268f5a473066053, 3684fe7a1cfe5285f3f71d4ba84ffab2, df218168bf83d26386dfd4ece7aef2d0, 44bd492dfb54107ebfe063fcbfbddff5, f627c30429d967082cdcf634aa735410, 597de376b1f80c06d501415dd973dcec
Email Addresses	datacentreback[@]msgsafe[.]io, moriartydata[@]onionmail[.]org
File Path	1.exe_, bild.exe_, \mimik\x32\mimik.exe, \mimik\x32\mimilib.dll, \mimik\x64\mimik.exe, \mimik\x64\mimilib.dll, webbrowserpassview.exe, mailpv.exe, vncpassview.exe, wirelesskeyview64.exe, bulletspassview64.exe, routerpassview.exe, mspass.exe, rdpv.exe, netpass64.exe, ns64.exe

References

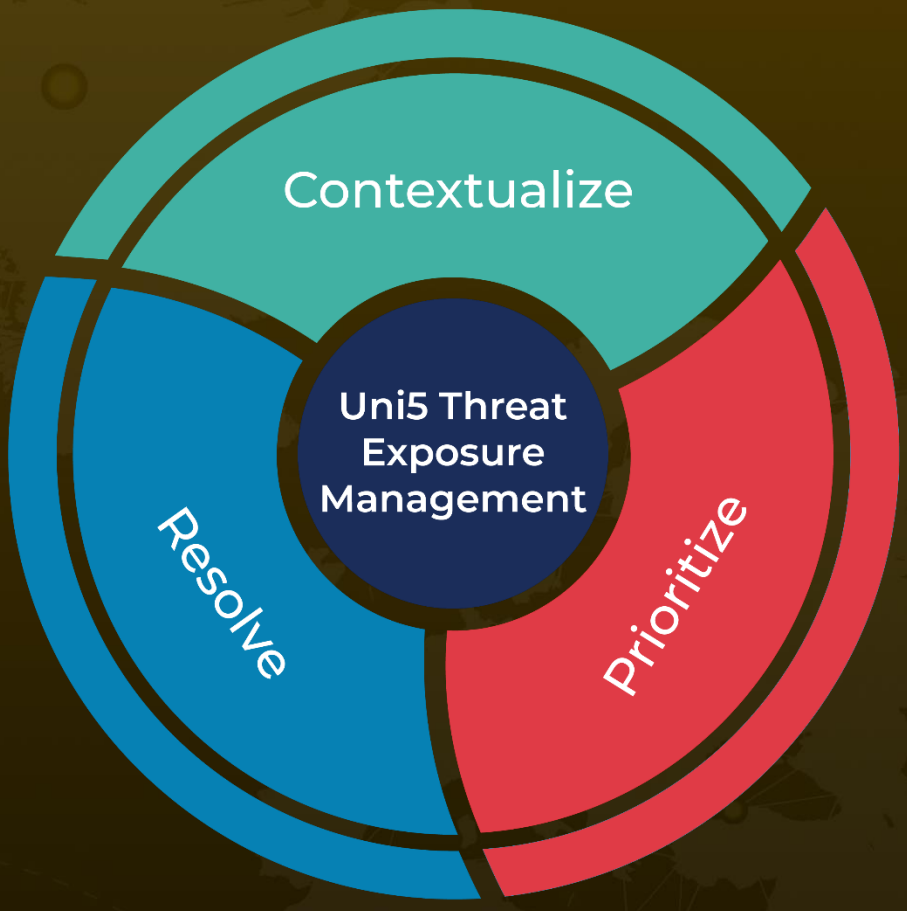
https://asec.ahnlab.com/en/54937/

https://www.hivepro.com/crysis-ransomware-a-long-standing-threat-with-a-new-twist/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 07, 2023 • 5:00 AM

More at www.hivepro.com